

PathRenameExtension

The destination string buffer must be long enough to hold the return file path

Sean Barnum, Cigital, Inc. [vita¹]

Copyright © 2007 Cigital, Inc.

2007-04-02

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 3854 bytes

Attack Category	<ul style="list-style-type: none">Malicious Input								
Vulnerability Category	<ul style="list-style-type: none">Buffer OverflowUnconditional								
Software Context	<ul style="list-style-type: none">File Path Management								
Location	<ul style="list-style-type: none">shlwapi.h								
Description	<p>The destination string buffer for PathRenameExtension() must be long enough to hold the return file path.</p> <p>The PathRenameExtension() routine changes the extension of a file, or adds one if not present. It appears to modify the path in place, so the buffer must be declared at least MAX_PATH in length (i.e., not exactly the size of the input string).</p>								
APIs	<table border="1"><thead><tr><th>Function Name</th><th>Comments</th></tr></thead><tbody><tr><td>PathRenameExtension</td><td>Src: 0, 1.</td></tr><tr><td>PathRenameExtensionA</td><td>Src: 0, 1. ASCII implementation</td></tr><tr><td>PathRenameExtensionW</td><td>Src: 0, 1. Unicode implementation</td></tr></tbody></table>	Function Name	Comments	PathRenameExtension	Src: 0, 1.	PathRenameExtensionA	Src: 0, 1. ASCII implementation	PathRenameExtensionW	Src: 0, 1. Unicode implementation
Function Name	Comments								
PathRenameExtension	Src: 0, 1.								
PathRenameExtensionA	Src: 0, 1. ASCII implementation								
PathRenameExtensionW	Src: 0, 1. Unicode implementation								
Method of Attack	If the path parameter is declared less than MAX_PATH in length, the attacker can provide a long extension that could overflow the in/out path parameter that is modified in place.								
Exception Criteria									
Solutions	<table border="1"><thead><tr><th>Solution Applicability</th><th>Solution Description</th><th>Solution Efficacy</th></tr></thead><tbody><tr><td>When PathRenameExtension() is called.</td><td>The first parameter, pszPath, must be at least large enough to hold the result. While it might</td><td>Effective.</td></tr></tbody></table>	Solution Applicability	Solution Description	Solution Efficacy	When PathRenameExtension() is called.	The first parameter, pszPath, must be at least large enough to hold the result. While it might	Effective.		
Solution Applicability	Solution Description	Solution Efficacy							
When PathRenameExtension() is called.	The first parameter, pszPath, must be at least large enough to hold the result. While it might	Effective.							

1. http://buildsecurityin.us-cert.gov/bsi/about_us/authors/35-BSI.html (Barnum, Sean)

	<p>be sufficient for the size to be the sum of the sizes of the inputs, best practice is to use a size of MAX_PATH characters in length.</p>				
Signature Details	<pre>BOOL PathRenameExtension(LPTSTR pszPath, LPCTSTR pszExt);</pre>				
Examples of Incorrect Code	<pre>TCHAR path[] = TEXT("AFileName"); // Buffer is too small LPTSTR pszPath = path; TCHAR ext[] = TEXT(".bat"); LPCTSTR pszExt = ext; if (!PathRenameExtension(pszPath, pszExt)) { handleError(); }</pre>				
Examples of Corrected Code	<pre>TCHAR path[MAX_PATH] = TEXT("AFileName"); // Buffer is correctly sized LPTSTR pszPath = path; TCHAR ext[] = TEXT(".bat"); LPCTSTR pszExt = ext; if (!PathRenameExtension(pszPath, pszExt)) { handleError(); }</pre>				
Source Reference	<ul style="list-style-type: none"> • http://msdn.microsoft.com/library/default.asp?url=/library/en-us/shellcc/platform/shell/reference/shlwapi/path/pathrenameextension.asp² 				
Recommended Resource					
Discriminant Set	<table border="1"> <tr> <td>Operating System</td> <td> <ul style="list-style-type: none"> • Windows </td> </tr> <tr> <td>Languages</td> <td> <ul style="list-style-type: none"> • C • C++ </td> </tr> </table>	Operating System	<ul style="list-style-type: none"> • Windows 	Languages	<ul style="list-style-type: none"> • C • C++
Operating System	<ul style="list-style-type: none"> • Windows 				
Languages	<ul style="list-style-type: none"> • C • C++ 				

Cigital, Inc. Copyright

Copyright © Cigital, Inc. 2005-2007. Cigital retains copyrights to this material.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

For information regarding external or commercial use of copyrighted materials owned by Cigital, including information about “Fair Use,” contact Cigital at copyright@cigital.com¹.

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

1. <mailto:copyright@cigital.com>